HWG | HARRIS, WILTSHIRE & GRANNIS LLP

1919 M STREET NW
SUITE 800
WASHINGTON DC 20036

TEL +1 202 730 1300
FAX +1 202 730 1301
HWGLAW.COM

ATTORNEYS AT LAW

April 4, 2017

BY ELECTRONIC FILING
Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Re: ***Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106**

Dear Ms. Dortch:

On March 31, 2017, Louise Tucker of iconectiv and Christopher J. Wright and Adrienne E. Fowler of Harris, Wiltshire & Grannis LLP met with Jennifer Tatel and Doug Klein of the Office of General Counsel and Madeleine Findley and Melissa Kirkel (via telephone) of the Wireline Competition Bureau. At this meeting, iconectiv re-iterated the urgent need for the Commission to quickly issue guidance on the continuing breadth of the fraud exemption.

The guidance should state that carriers may—at their own option and without prior customer consent—share customer proprietary network information ("CPNI") with third party fraud prevention partners to prevent and respond to fraud that uses telecommunications networks and harms telecommunications customers, such as account takeover fraud ("ATO"), even if:

- the party receiving the CPNI is not a carrier;
- the sharing is not limited to individual accounts and occurs on an ongoing basis, rather than only in response to particular instances of suspected fraud;
- other institutions also benefit from the fraud prevention; and/or
- the customer has been ported to another carrier.

The statutory text of Section 222 clearly allows sharing under these circumstances, as the Commission affirmed first in 1999 and then again when it passed its recent Privacy Order.[1]

Current regulatory uncertainty places iconectiv's ATO prevention and response efforts in jeopardy. Congress recently passed—and, between the time of our meeting and the filing of this notice, President Trump signed—a Congressional Review Act ("CRA") resolution that prevents the Privacy Order from having any effect. This creates industry-wide uncertainty, including over

[1] Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., Report & Order, FCC No. 16-148, WC Docket No. 16-106 (rel. Nov. 2, 2016) ("Privacy Order").

whether the FCC's well established support for sharing CPNI in order to prevent fraud remains in effect, simply because the Commission re-iterated this support in the Privacy Order.

The FCC can and should dispel the uncertainty in the fraud context. The plain text of the statute allows use and sharing of CPNI to prevent and respond to fraud. The CRA simply nullifies the Privacy Order, not the statutory text or prior FCC rules allowing for the use and disclosure of CPNI to prevent and respond to fraud. And ATO presents a pressing and urgent threat to telecommunications customers, which the Commission should address now.

I. Background on ATO

Among other security solutions, iconectiv is working to protect mobile consumers from ATO. In ATO, a criminal hijacks a phone number (frequently by impersonating a customer and having the number ported to another carrier) and associates it with the criminal's device. The thief can then request a password reset for the consumer's email account, bank account, online shopping account, cryptocurrency account, or any other account that uses the customer's phone number to verify the customer's identity. For multi-factor authentication, many companies will send a one-time password to the customer's phone number on the theory that only the customer will have possession of his or her own phone. But since the phone number has been hijacked, that one-time password is sent to the *thief's* phone. The thief can then use the one-time password to gain control over the consumer's account.

The scale and severity of ATO fraud has grown significantly in the past few years. Reports of ATO to the Federal Trade Commission more than doubled between January 2013 and January 2016.[2] According to a recent article in Forbes, criminals who are "incredibly sophisticated and incredibly organized" perpetuate these frauds.[3] They work in coordination and use automated procedures, enabling them to steal quickly. For example, in a recent incident, criminals stole approximately thirty of the same victim's accounts within seven minutes.[4] Even the most tech-savvy and fraud-aware can have difficulty avoiding this type of fraud. As companies protect their customers using mobile identity as a form of multi-factor authentication, the number of accounts vulnerable to ATO will only continue to grow. Telecommunications customers, fraud prevention companies, companies offering consumer accounts, and carriers *all* stand to gain from improved solutions to combat ATO.

To implement these solutions, however, iconectiv and any other similarly situated fraud prevention companies need access to information protected by Section 222 on an ongoing

---

[2] Lorrie Cranor, *Your Mobile Phone Account Could Be Hijacked by an Identity Thief*, TECH@FTC BLOG (June 7, 2016, 11:38 AM), https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief.

[3] Laura Shin, *Hackers Have Stolen Millions of Dollars in Bitcoin – Using Only Phone Numbers*, FORBES (Dec. 20, 2016, 1:59 PM), http://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers.

[4] *Id.*

basis—not a limited subset of information in response to a suspected security incident, or after a consumer realizes he or she needs this protection and grants consent. This is because some of the best indicators of ATO, including calling patterns, qualify as CPNI. And in order to find out what *abnormal* customer behavior is (in the event of a suspected security incident), iconectiv must have access to data demonstrating what *normal* customer behavior is. Moreover, because ATO is often accomplished through the fraudulent porting of a number from one carrier to another, cross-network access to CPNI about carriers' current and former customers will provide the best dataset to combat ATO.

II. The Fraud Exception

The plain statutory text of Section 222 allows the use and sharing of CPNI without customer consent in order to combat ATO, even if:

- the party receiving the CPNI is not a carrier;
- the sharing is not limited to individual accounts and occurs on an ongoing basis, rather than only in response to particular instances of suspected fraud;
- other institutions also benefit from the fraud prevention; and/or
- the customer has been ported to another carrier.

The statute states that "*nothing*" in Section 222, including the provisions dealing with consent, "prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information . . . to protect users of [telecommunications] services . . . from fraudulent, abusive, or unlawful use of, or subscription to, such services."[5] It contains no limits on to whom a carrier can disclose protected information. Congress did not limit this exception to specific incident response. The plain text allows any sharing "to protect users," regardless of whether the sharing occurs on an ongoing basis or whether other actors benefit from consumers receiving fraud protection. And there is no statutory limit saying a customer can no longer be protected after his or her number has been ported.

The FCC first affirmed in 1999 that it read the fraud exception to mean exactly what it says. In 1999, Comcast asked the Commission to clarify that it could use, disclose, or permit access to CPNI without customer approval, on an ongoing basis in connection with fraud prevention programs, even after the customer had ported to another carrier.[6] The FCC granted Comcast's request, stating that "Section 222(d)(2) *on its face* permits the use of CPNI in connection with fraud prevention programs, and does not limit such use of CPNI that is generated during the customer's period of service to any period of time."[7]

---

5 47 U.S.C. § 222(d) (emphasis added).

6 Telecomms. Carriers' Use of CPNI & Other Customer Info., 64 Fed. Reg. 53242, 53259 (Oct. 1, 1999).

7 *Id.* (emphasis added).

In the Privacy Order, the FCC re-iterated its commitment to giving full effect to Congress's words in Section 222(d)(2). It affirmed that Section 222(d)(2) permits "carriers to use, disclose, and permit access to CPNI to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services without obtaining specific customer approval."[8] It re-iterated its 1999 conclusion that the fraud exemption does not cover the use or sharing of CPNI only at the time a fraudulent incident occurs. Rather, the fraud exemption "encompass[es] not only actions taken to combat immediate security threats, but also uses and sharing to research and develop [(1)] network and cybersecurity defenses . . . [and (2)] new techniques and technologies for addressing fraud and abuse."[9] And it stated that "addressing fraud and abuse [pursuant to Section 222(d)(2)] may require internal use of [CPNI], but also disclosures to third-party researchers and other collaborators."[10]

III. Authority for Clarification

Uncertainty about whether the CRA forces the FCC to change its regulatory approach toward the fraud exception could impede fraud prevention providers' and innovators' access to CPNI and put consumers at risk. In light of the large and growing threat that ATO poses, the Commission should act *quickly* to clarify that Section 222 allows the use and sharing of CPNI without customer consent in order to combat ATO.

Where Congress enacts a joint resolution disapproving of an agency rule under the CRA, and the president signs it, the rule does "not take effect (or continue [in effect])."[11] The joint resolution at issue here provides "[t]hat Congress disapproves the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services' (81 Fed. Reg. 87274 (December 2, 2016)), and such rule shall have *no force or effect*."[12] Because the Privacy Order no longer has force or effect, the FCC's regulation of CPNI continues as if the Privacy Order had never passed. Before the passage of the Privacy Order, carriers could use, share, or disclose information on an ongoing basis in order to combat ATO. Thus, they may continue to do so now. In this time of great upheaval in the Commission's Section 222 regulations, however, the Commission should reassure the industry that this is the case.

---

8 Privacy Order ¶ 212.

9 *Id.* ¶ 214.

10 *Id.*

11 5 U.S.C. § 801(b)(1).

12 S.J. Res. 34, 115th Cong. (2017) (emphasis added).

Should you have any questions, please contact the undersigned.

Respectfully submitted,

/s/ Christopher J. Wright
Christopher J. Wright
Adrienne E. Fowler
Counsel to iconectiv

cc: Meeting attendees